CLAIMS

I claim:

1. A method for managing network access of a device, which is a capable of communicating with one or more networks, comprising the steps of:

storing a network access parameter in a secure token local to said device and

determining if said network access parameter has been met or exceeded.

2. The method of claim 1, wherein said network access parameter is selected from the group consisting of:

maximum number of connections to said network, time of day, period of time, day in week, date, range of dates, maximum period of time spent connected to said network, device address, subnet ID, and LAN ID.

3. The method of claim 1, further comprising the step of

storing one or more additional network access parameters in said secure token.

4. The method of claim 3, further comprising the steps of:

determining if said one or more additional access parameters have been met or exceeded and

denying access to said network if any of said network access parameters have been met or exceeded.

5. The method of claim 3, further comprising the steps of:

determining if said one or more additional access parameters have been met and

restricting access to a portion of said network if any of said network access parameters have been met or exceeded.

6. The method of claim 5, wherein said portion of said network includes a server and said method further comprising the steps of:

authorizing additional usage of said network at said server and

modifying said network access parameter.

7. The method of claim 6, wherein said step of authorizing comprises the step of receiving payment for said additional usage of said network.

8. The method of claim 3, further comprising the step of

determining if said one or more additional access parameters has been met and

allowing access to said network if all of said network access parameters has not been met.

9. The method of claim 3, wherein at least one of said network access parameters is associated with a first network and at least one of said remaining network access parameters is associated with a second network.

10. The method of claim 1, wherein said network is an 802.11 network.

11. The method of claim 10, wherein said secure token is implemented through a USB adapter.

12. The method of claim 10, wherein current time is received from an access point on said 802.11 network.

13. The method of claim 1, wherein said step of determining is performed by a usage application executed at said device.

14. The method of claim 13, wherein said usage application is stored within said secure token.

15. The method of claim 1, wherein said secure token is unique to said device.

16. The method of claim 1, wherein said secure token comprises authentication information for authenticating said device with said network.

17. The method of claim 1, wherein said network access parameter is pre-stored within said secure token.

18. A physical token comprising:

a communications interface for communicating data to and from said physical token and

a storage including at least one access parameter associated with a first network.

19. The physical token of claim 18, wherein said at least one access parameter is part of a first usage plan for said first network.

20. The physical token of claim 19, wherein said storage further includes

a usage application for tracking and enforcing usage of said first network according to said first usage plan.

21. The physical token of claim 18, further comprising

an adapter for connecting said physical token to a device capable of communicating with said first network.

22. The physical token of claim 18, wherein said storage further includes

at least one access parameter associated with a second network.

23. The physical token of claim 18, wherein said storage further includes authentication information for authenticating said device with said first network.